Las autoridades policiales han informado sobre la desarticulación de una red criminal internacional que utilizaba una plataforma de phishing para desbloquear teléfonos móviles robados o extraviados.

La plataforma de phishing como servicio (PhaaS), conocida como iServer, se estima que ha afectado a más de 483,000 personas en todo el mundo, con las principales víctimas en Chile (77,000), Colombia (70,000), Ecuador (42,000), Perú (41,500), España (30,000) y Argentina (29,000).

> *«Las víctimas son mayoritariamente ciudadanos hispanohablantes de países europeos, norteamericanos y sudamericanos»,* afirmó Europol en un comunicado de prensa.

La operación, denominada Kaerb, contó con la colaboración de cuerpos policiales y judiciales de España, Argentina, Chile, Colombia, Ecuador y Perú.

Durante la acción conjunta que se llevó a cabo entre el 10 y el 17 de septiembre, se arrestó a un ciudadano argentino que había estado desarrollando y gestionando el servicio PhaaS desde 2018.

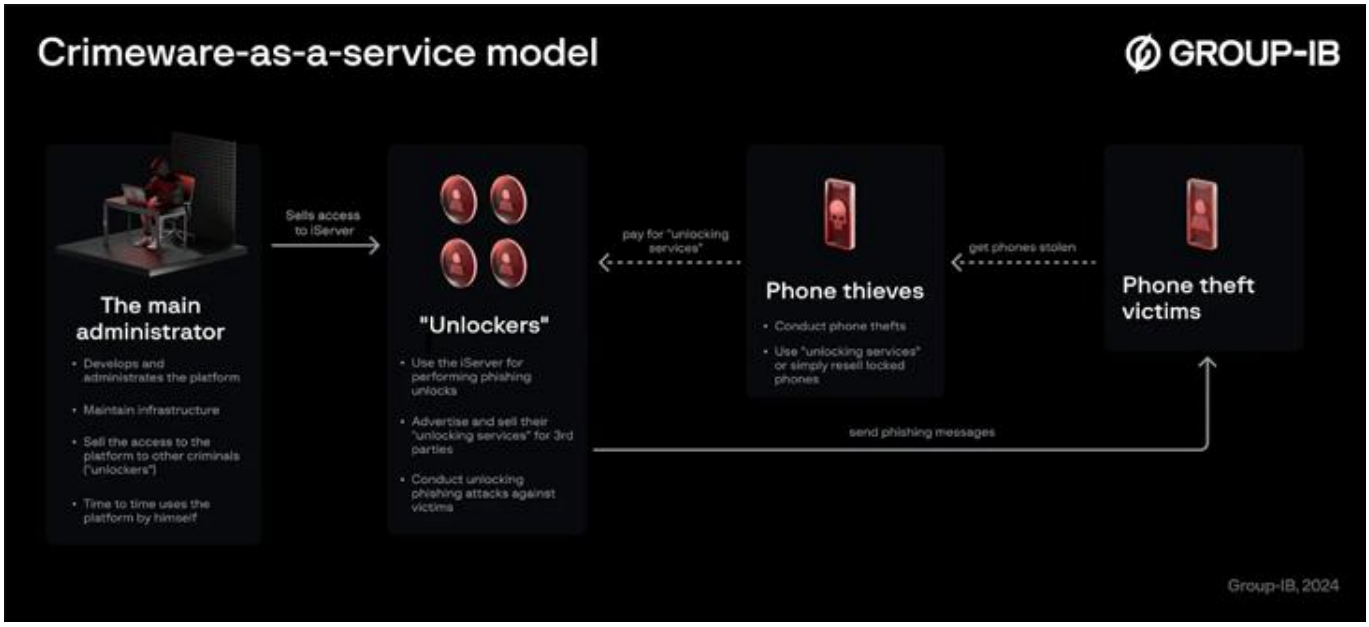
En total, la operación resultó en 17 detenciones, 28 allanamientos y la confiscación de 921 objetos, incluidos teléfonos móviles, dispositivos electrónicos, vehículos y armas. Se estima que hasta ahora se han desbloqueado aproximadamente 1.2 millones de teléfonos móviles.

> *«Aunque iServer era principalmente una plataforma automatizada de phishing, su especialización en la obtención de credenciales para desbloquear dispositivos robados la hacía diferente de las ofertas tradicionales de phishing como servicio»*, explicó Group-IB.

Según esta empresa con sede en Singapur, iServer ofrecía una interfaz web que permitía a delincuentes de baja especialización, conocidos como «*desbloqueadores*«, extraer contraseñas de dispositivos y credenciales de usuarios en plataformas móviles basadas en la nube, permitiéndoles desactivar el Modo Perdido y desbloquear los dispositivos.

El administrador de esta red criminal ofrecía acceso a estos desbloqueadores, quienes, a su vez, usaban iServer no solo para realizar desbloqueos mediante phishing, sino también para vender estos servicios a terceros, como ladrones de teléfonos.

Los desbloqueadores también eran responsables de enviar mensajes falsos a las víctimas de robos de teléfonos, buscando obtener información que les permitiera acceder a esos dispositivos. Lo lograban enviando SMS que instaban a los usuarios a localizar su teléfono perdido mediante un enlace.



Esto activaba una cadena de redireccionamientos que finalmente conducía a la víctima a una página web en la que se les pedía que introdujeran sus credenciales, el código de acceso del dispositivo y los códigos de autenticación de dos factores (2FA), los cuales luego se usaban

para acceder ilegalmente al dispositivo, desactivar el Modo Perdido y desvincular el dispositivo de la cuenta del propietario.

> *«iServer automatizaba la creación y distribución de páginas de phishing que imitaban a las principales plataformas móviles basadas en la nube, utilizando implementaciones únicas que aumentaban su eficacia como herramienta de cibercrimen»,* explicó Group-IB.

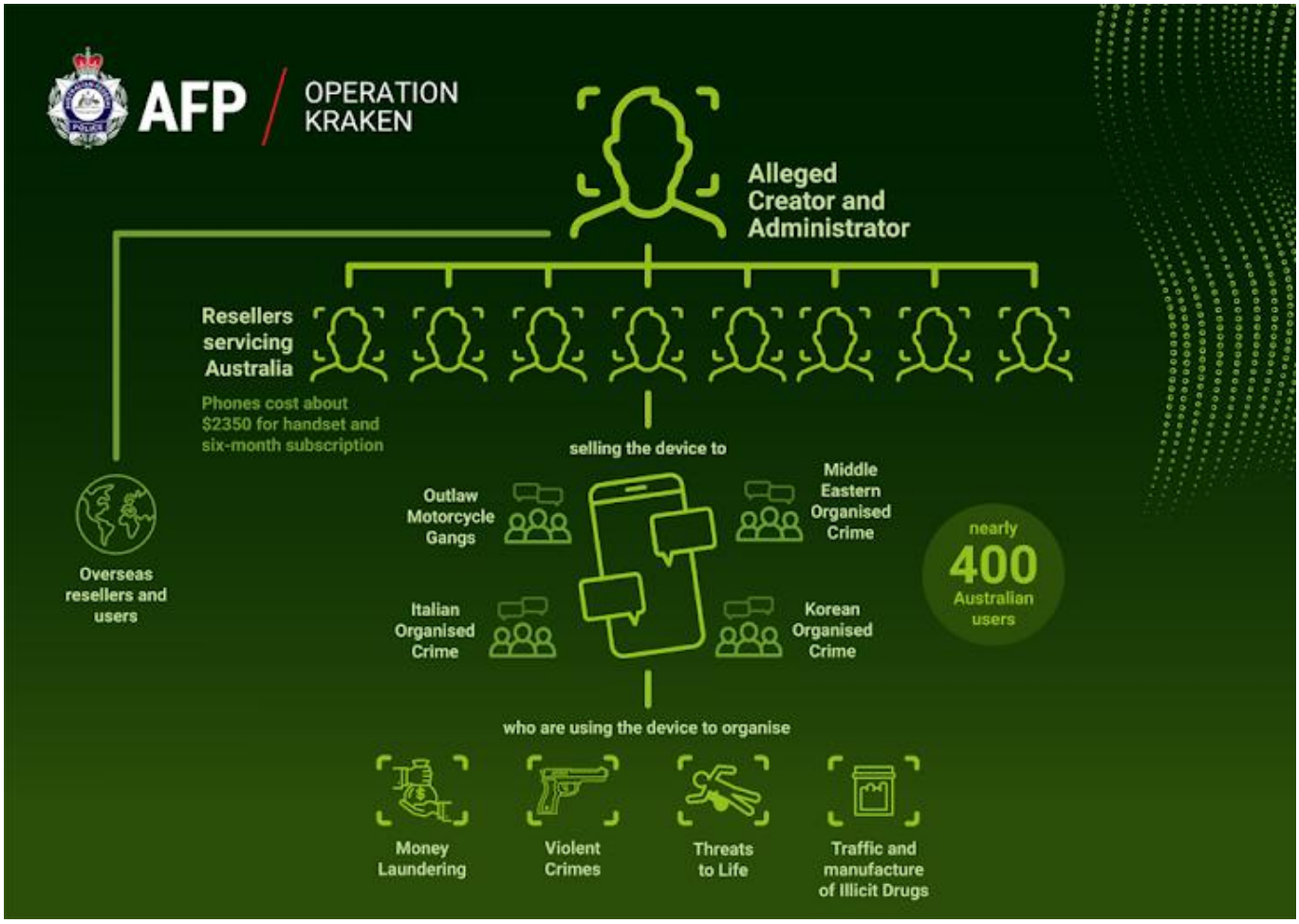
Plataforma Ghost desmantelada en operación global

Europol y la Policía Federal Australiana (AFP) han informado sobre el desmantelamiento de una red de comunicaciones cifradas conocida como Ghost («www.ghostchat[.]net«), la cual facilitaba el crimen organizado y grave a nivel internacional.

La plataforma, que se ofrecía con un teléfono Android personalizado por aproximadamente $1,590 con una suscripción de seis meses, se utilizaba para llevar a cabo diversas actividades ilegales, como el tráfico de drogas, el lavado de dinero y actos de extrema violencia. Es la última en una serie de servicios similares, como Phantom Secure, EncroChat, Sky ECC y Exclu, que también han sido cerrados por motivos similares.

> *«El sistema usaba tres estándares de cifrado y permitía enviar un mensaje con un código especial que activaba la autodestrucción de todos los mensajes en el dispositivo de destino. Esto permitía a las redes criminales comunicarse de forma segura, evitar la detección, contrarrestar las medidas forenses y coordinar sus actividades ilegales a través de las fronteras»,* explicó Europol.

Se calcula que miles de personas utilizaron esta plataforma, con alrededor de 1,000 mensajes intercambiados diariamente antes de su cierre.



La investigación, que comenzó en marzo de 2022, resultó en el arresto de 51 personas: 38 en Australia, 11 en Irlanda, una en Canadá y una en Italia, vinculada a la mafia italiana Sacra Corona Unita.

Entre los detenidos destaca un hombre de 32 años de Sídney, Nueva Gales del Sur, acusado de crear y administrar Ghost como parte de la Operación Kraken, junto a otros individuos acusados de usar la plataforma para traficar cocaína y cannabis, distribuir drogas y fabricar un falso complot terrorista.

Se cree que el administrador, Jay Je Yoon Jung, comenzó esta operación criminal hace nueve

años, obteniendo millones de dólares en ganancias ilícitas. Fue arrestado en su casa en Narwee. La operación también permitió el desmantelamiento de un laboratorio de drogas en Australia, además de la confiscación de armas, drogas y €1 millón en efectivo.

La AFP informó que lograron infiltrarse en la infraestructura de la plataforma, llevando a cabo un ataque de cadena de suministro de software al modificar el proceso de actualización del sistema, lo que les permitió acceder al contenido de 376 teléfonos activos en Australia.

> *«El panorama de las comunicaciones cifradas se ha vuelto más fragmentado debido a las recientes acciones de las fuerzas de seguridad que han atacado plataformas utilizadas por redes criminales»*, destacó Europol.
>
> *«En respuesta, los criminales ahora recurren a herramientas de comunicación menos conocidas o personalizadas que ofrecen diferentes niveles de seguridad y anonimato. También están adoptando aplicaciones de comunicación populares para diversificar sus métodos.»*

La agencia también subrayó la importancia de acceder a las comunicaciones entre sospechosos para combatir delitos graves, e instó a las empresas privadas a garantizar que sus plataformas no se conviertan en refugios seguros para delincuentes, ofreciendo acceso legal a los datos *«bajo supervisión judicial y respetando plenamente los derechos fundamentales.»*

Alemania cierra 47 intercambios de criptomonedas

Estas acciones coinciden con el cierre en Alemania de 47 servicios de intercambio de criptomonedas que facilitaban actividades de lavado de dinero para ciberdelincuentes, incluidos grupos de ransomware, vendedores en la darknet y operadores de botnets. La operación fue llamada Final Exchange.

Se acusa a estos servicios de no implementar programas de Conozca a su Cliente (KYC) ni políticas de prevención del lavado de dinero, y de ocultar deliberadamente el origen de fondos ilícitos, permitiendo que el cibercrimen prosperara. No se informaron arrestos.

> *«Los servicios de intercambio permitían realizar transacciones sin necesidad de registrarse ni verificar la identidad de los usuarios. La oferta estaba dirigida a intercambiar criptomonedas de forma rápida, fácil y anónima para ocultar su origen»,* explicó la Oficina Federal de Policía Criminal (Bundeskriminalamt).

El Departamento de Justicia de EE. UU. acusa a dos por estafa de criptomonedas de $230 millones

Como parte de los esfuerzos para combatir el cibercrimen, el Departamento de Justicia de los EE. UU. (DoJ) anunció el arresto y la acusación de dos personas por conspiración para robar y lavar más de $230 millones en criptomonedas de una víctima en Washington D.C.

Malone Lam, de 20 años, y Jeandiel Serrano, de 21, junto con otros cómplices, supuestamente cometieron robos de criptomonedas desde al menos agosto de 2024, accediendo a las cuentas de las víctimas y lavando los fondos a través de diversos intercambios y servicios de mezcla.

Las ganancias ilícitas se utilizaron para financiar un estilo de vida lujoso, incluyendo viajes internacionales, visitas a clubes nocturnos, autos de lujo, relojes, joyas, bolsos de diseñador y casas de alquiler en Los Ángeles y Miami.

> *«Lavaron los fondos moviéndolos a través de varios mezcladores e intercambios, usando 'cadenas de pelado', billeteras temporales y redes privadas virtuales (VPN) para ocultar sus verdaderas identidades»*, indicó el DoJ.